Collusive Eavesdropping in Interference Alignment (IA)-Based Wireless Networks

Nan Zhao, *Senior Member, IEEE,* F. Richard Yu, *Senior Member, IEEE,* Yunfei Chen, *Senior Member, IEEE,* and Victor C.M. Leung, *Fellow, IEEE*

***Abstract*—Interference alignment (IA) can be secure due to the fact that the received signal of a targeted user at the eavesdropper may be embedded by interference from other concurrent users. However, when some malicious users inside the network cooperate to eavesdrop one specific user, the network will not be secure any more. Thus, we focus on the eavesdropping attacks, and propose a novel collusive eavesdropping scheme (CES) in a K-user IA-based network. In this scheme, one user is eavesdropped by an eavesdropper with the aid of the other $(K-2)$ users. To perform passive eavesdropping without being noticed by the targeted user, the precoding and decoding matrices of the eavesdropper and its cooperators are re-designed, and some of the cooperators sacrifice their own quality of transmission to help the eavesdropper meet the feasibility condition. Therefore, the feasibility condition of CES is derived, based on which the minimal number of low-quality cooperators and the maximal number of receiving antennas at each user are obtained. The received power of eavesdropping is analyzed with different numbers of antennas at each receiver, which also affects the eavesdropping performance. Extensive simulation results are provided to show the effectiveness of CES.**

***Index Terms*—Collusive eavesdropping, feasibility conditions, interference alignment, MIMO, wireless security.**

I. Introduction

INTERFERENCE is a fundamental problem of wireless networks, and it will become more and more severe in future wireless systems due to the tremendous expansion of mobile devices and data traffic [2]. Thus, interference management is a key issue in modern wireless communications, and interference alignment (IA) is one of the promising solutions [3], [4]. In the spatial IA-based wireless networks, the precoding matrices are cooperatively designed to constrain the interference into certain subspace at the unintended receivers, and thus, the desired signal can be recovered in an interference-free subspace by the decoding matrices at each receiver [5]. Although IA can achieve excellent performance in approaching the sum capacity of wireless interference networks at high signal-to-noise ratio (SNR), there are still some practical challenges to be solved, which have attracted a lot of interest from both academia and industry [6]. When there exist plenty of users in IA-based networks, the closed-form solutions of IA are difficult to obtain. Thus, some iterative and distributed algorithms were proposed for IA based on the reciprocity of wireless networks in [5]. To determine whether or not an IA problem is solvable, its feasibility conditions were analyzed and derived in [7], [8]. When SNR becomes lower, the sum rate of IA-based networks may fall short of the theoretical maximum, and a lot of research effort has been concentrated on this aspect [5], [9], [10]. We have also worked on this issue, and utilized opportunistic communications and power allocation to improve the quality of service (QoS) for IA-based networks [11]–[13]. Accurate channel state information (CSI) of the whole network should be available at all the nodes to achieve IA, and several methods were proposed to reduce the CSI overhead of IA-based networks [10], [12], [14]–[20].

On the other hand, secure information transfer is still a critical challenge in wireless networks, and wireless security is becoming more and more important [21], [22]. In the physical layer of wireless networks, one of the key threats from adversarial users is eavesdropping, which is caused by the broadcast nature of wireless channels [23]. When eavesdropping is considered in wireless networks, we should guarantee that the confidential data can only be recovered by the legitimate receiver rather than eavesdroppers [24]. Some pioneering research was done on eavesdropping [25] in which the wiretap model was introduced and the concept of secrecy capacity was defined. Following this direction, plenty of anti-eavesdropping schemes have emerged in recent years, and some prevalent methods are zero-forcing the signal at the eavesdropper by beamforming, generating artificial noise (AN) to disrupt the eavesdropping, and enhancing wireless secrecy via cooperative transmission [24], [26]–[33], etc.

When the security of IA-based networks is considered, IA seems to be secure, due to its inherent property of aligning interferences in certain subspaces, which is demonstrated in Fig. 1 [34]. We analyze the security of IA as follows.

External Jammer: When there exists an adversarial jammer outside the IA-based network that aims to disrupt the transmission of IA users, more antennas can be equipped to align the interferences among users in the same subspace as the jamming signal [35], [36]. Thus, the jamming signal can be eliminated effectively along with the interference.

Manuscript received October 11, 2016; revised January 17, 2017, May 6, 2017; accepted May 25, 2017. This research was supported in part by the Xinghai Scholars Program. This paper was presented in preliminary form at the 2017 IEEE 85th Vehicular Technology Conference (VTC2017-Spring) [1]. The associate editor coordinating the review of this paper and approving it for publication was B. Hamdaoui. *(Corresponding author: Nan Zhao.)*

N. Zhao is with the School of Inform. and Commun. Eng., Dalian University of Technology, Dalian, Liaoning, P. R. China (email: zhaonan@dlut.edu.cn).

F.R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, K1S 5B6, Canada (email: richard.yu@carleton.ca).

Y. Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

V.C.M. Leung is with the Department of Electrical and Computer Engineering, the University of British Columbia, Vancouver, BC, V6T 1Z4, Canada (email: vleung@ece.ubc.ca).

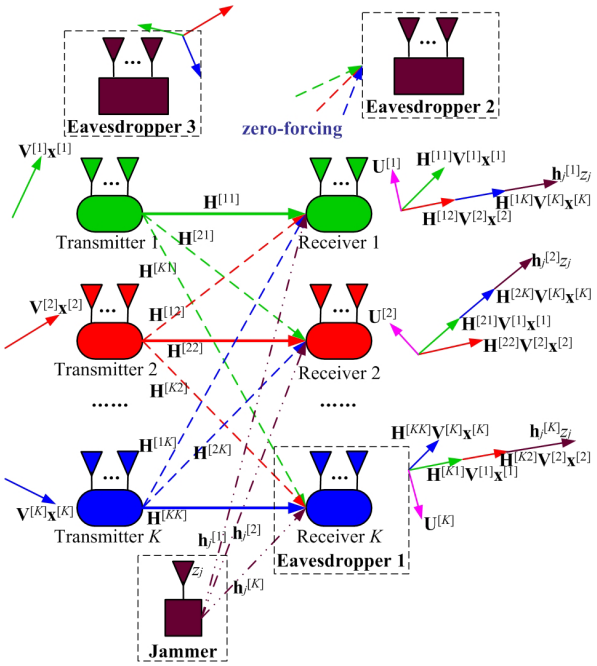

Fig. 1. Security analysis of IA. Four cases are considered, i.e., the external jammer, the internal eavesdropper, the external eavesdropper with CSI available, and the external eavesdropper with CSI unknown.

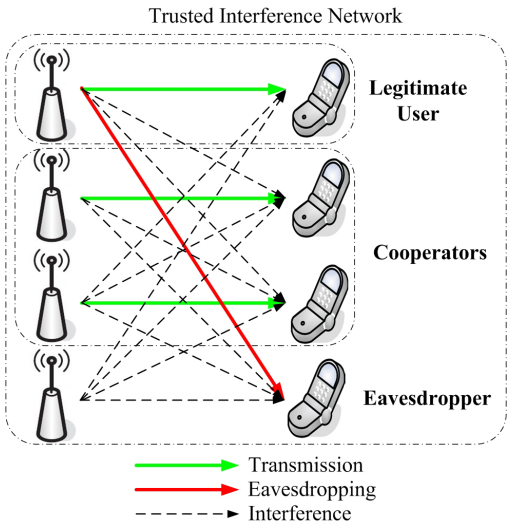

Fig. 2. Pictorial illustration of the CES in IA-based networks.

Internal Eavesdropper: When there exists an eavesdropper inside the IA-based network (the Kth receiver in Fig. 1), it aims to obtain the information transmitted by other users secretly. It is difficult to achieve this, because the signals from other users overlap in the same subspace, and the targeted information cannot be recovered successfully.

External Eavesdropper, CSI known: Assume that there exists an eavesdropper outside the IA-based network (eavesdropper 2 in Fig. 1), and its CSI is known by the IA network. The IA users can perform zero-forcing on their transmitted signals at the eavesdropper and align the interference at each user simultaneously through cooperative precoding using more antennas.

External Eavesdropper, CSI unknown: When the CSI of eavesdropper outside the IA-based network (eavesdropper 3 in Fig. 1) is unknown to the legitimate users, it might be possible to perform eavesdropping. However, when plenty of users exist, the targeted signal is embedded in the interference from other users, and the eavesdropping efficiency can be limited. Besides, AN can also be created to further prevent eavesdropping [37], without affecting the legitimate network.

From the above analysis, IA is secure on the condition that all the users in the network can be trusted. However, when there exist some adversarial untrusted IA users inside the network, it becomes much more vulnerable to attacks through collusive eavesdropping. Thus, in this paper, we propose a collusive eavesdropping scheme (CES) in IA-based wireless networks as depicted in Fig. 2, in which the internal eavesdropper can eavesdrop the information of the legitimate user with the help of some collusive cooperators, and without perception of the user being eavesdropped. The motivations and contributions of this work are recapitulated as follows.

- In contrast to the existing research of physical layer security on anti-eavesdropping methods, in this paper, we concentrate on the eavesdropping attacks inside multi-user IA-based networks. This work has two motivations. First, it provides a feasible method to penetrate the IA-based networks and perform collusive eavesdropping, when these IA users can no longer be trusted. In particular, it can be utilized in the cognitive radio or device-to-device (D2D) networks, in which the unlicensed or D2D users can act as the eavesdropper and cooperators, to collusively eavesdrop the transmission of the licensed or cellular user. Second, the proposed CES can provide a potential threat to IA-based networks, and its analysis will help us to prevent this kind of eavesdropping attack when we design the network, e.g., increasing the number of N as analyzed in Section IV.
- In the proposed CES based on a feasible IA network, a certain user is eavesdropped by one eavesdropper in the network, and all the other users act as cooperators to help the eavesdropper. In order not to be noticed by the legitimate user, the number of users and antennas should not be changed in the CES, and only the precoding and decoding matrices of the eavesdropper and cooperators need to be re-designed.
- To perform collusive eavesdropping, some of the cooperators need to sacrifice their own QoS of transmission to help the eavesdropper, and the feasibility condition of the proposed CES is presented, through which the minimal number of the low-SINR cooperators and the maximal number of receiving antennas at each receiver are derived.
- In addition to the feasibility, which will determine the interference leakage, the received power of eavesdropping will also affect its performance, due to the fact that the power is varying with different numbers of receiving antennas even when the scheme is feasible. Thus the received power of eavesdropping is analyzed with different numbers of receiving antennas at each receiver.

TABLE I
LIST OF MATHEMATICAL NOTATIONS

Notation	Definition
$\mathbf{0}_{M\times N}$	$M \times N$ zero matrix
$\mathbf{I}_N$	$N \times N$ identity matrix
$\mathbb{E}(\cdot)$	Expectation
$\mathbb{C}^{M\times N}$	The space of complex $M \times N$ matrices
$\mathcal{CW}_d(n, \mathbf{\Sigma})$	Wishart distribution of an $d \times d$ matrix with n degrees of freedom and a covariance matrix $\mathbf{\Sigma}$
$\mathbf{A}^\dagger$	Conjugate transpose of matrix $\mathbf{A}$
$Tr(\mathbf{A})$	Trace of matrix $\mathbf{A}$
$\nu_i[\mathbf{A}]$	Eigenvector corresponding to the ith smallest eigenvalue of matrix $\mathbf{A}$
$\mathbf{A}_{\star l}$	The lth column of matrix $\mathbf{A}$
$\mathcal{CN}(\mathbf{a}, \mathbf{A})$	Complex Gaussian distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$

The rest of this paper is arranged as follows. In Section II, we describe the system model. The collusive eavesdropping scheme in IA networks is proposed, and the iterative algorithm to achieve CES is designed in Section III. In Section IV, the performance and feasibility condition of the CES is analyzed. Simulation results are discussed in Section V, and finally, conclusions are made in Section VI. Table I provides a list for the mathematical notations used in this paper.

II. SYSTEM MODEL

In a K-user interference network with $d^{[k]}$ independent data streams transmitted by the kth user, $M^{[k]}$ and $N^{[k]}$ antennas are equipped at the kth transmitter and receiver, respectively. IA is adopted to avoid the interference among users, and the received signal of the kth user in the network can be expressed as

$$\mathbf{y}^{[k]} = \sum_{j=1}^{K} \mathbf{U}^{[k]\dagger}\mathbf{H}^{[kj]}\mathbf{V}^{[j]}\mathbf{x}^{[j]} + \mathbf{U}^{[k]\dagger}\mathbf{n}^{[k]}, \tag{1}$$

where $\mathbf{H}^{[kj]} \in \mathbb{C}^{N^{[k]}\times M^{[j]}}$ is the channel matrix between the jth transmitter and the kth receiver, each element of which is independent and identically distributed (i.i.d.) and follows $\mathcal{CN}(0, 1)$. $\mathbf{V}^{[k]} \in \mathbb{C}^{M^{[k]}\times d^{[k]}}$ and $\mathbf{U}^{[k]} \in \mathbb{C}^{N^{[k]}\times d^{[k]}}$ are unitary precoding and decoding matrices of the kth user, respectively, which are exploited to constrain the interferences into certain subspaces to recover the desired signal free of interference. $\mathbf{V}^{[k]\dagger}\mathbf{V}^{[k]} = \mathbf{I}_{d^{[k]}}$ and $\mathbf{U}^{[k]\dagger}\mathbf{U}^{[k]} = \mathbf{I}_{d^{[k]}}$. $\mathbf{x}^{[k]}$ is the signal vector of $d^{[k]}$ data streams transmitted by the kth user with power $P_t^{[k]}$, i.e., $\mathbb{E}\left[\left\|\mathbf{x}^{[k]}\right\|^2\right] = P_t^{[k]}$. $\mathbf{n}^{[k]} \in \mathbb{C}^{N^{[k]}\times 1} \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2\mathbf{I}_{N^{[k]}})$ is the additive white Gaussian noise (AWGN) vector at the kth receiver.

To make IA feasible to achieve, the following conditions should be satisfied as

$$\mathbf{U}^{[k]\dagger}\mathbf{H}^{[ki]}\mathbf{V}^{[i]} = \mathbf{0}_{d^{[k]}\times d^{[i]}},\ \forall i \neq k, \tag{2}$$

$$\operatorname{rank}\left(\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\right) = d^{[k]},\ \forall k \in \{1, 2, \ldots, K\}. \tag{3}$$

Because the channel matrices do not have any special structure, only the condition (2) should be considered when calculating the solutions of IA, and (3) will be automatically satisfied almost surely. Thus, the interference among users is effectively eliminated, and the recovered signal of the kth user in (1) becomes

$$\mathbf{y}^{[k]} = \overline{\mathbf{H}}^{[kk]}\mathbf{x}^{[k]} + \overline{\mathbf{n}}^{[k]}, \tag{4}$$

where

$$\overline{\mathbf{H}}^{[kk]} \triangleq \mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}, \tag{5}$$

$$\overline{\mathbf{n}}^{[k]} = \mathbf{U}^{[k]\dagger}\mathbf{n}^{[k]}. \tag{6}$$

If the symmetric IA networks are considered, all the users are assumed to have the same parameters for simplicity in the rest of this paper, i.e., $M^{[k]} = M$, $N^{[k]} = N$ and $d^{[k]} = d$ for all the IA users[1].

From the analysis in Fig. 1, IA seems secure, on the condition that all the users in the IA-based network can be trusted. However, when some IA users in the network aim to eavesdrop a certain user collusively, it becomes vulnerable to be attacked with a much lower security level due to the exchange of global CSI in the network. In the rest of this paper, we will focus on this potential threat arising in IA-based networks.

III. COLLUSIVE EAVESDROPPING IN IA-BASED NETWORKS

In this section, the CES in IA-based wireless networks is proposed, and an iterative algorithm for achieving this scheme is designed.

A. Collusive Eavesdropping Scheme in IA-Based Networks

As analyzed in Fig. 1, the information transmitted in the IA-based network cannot be easily eavesdropped by a certain unintended IA user. Nevertheless, when one user is eavesdropped collusively by all the others, it can be achieved. Thus, we propose a novel collusive eavesdropping scheme, CES, in IA-based networks, which is illustrated in Fig. 3.

Without loss of generality, we assume that the 1st user is eavesdropped by the Kth user, with the help of the 2nd to the $(K-1)$th users. Thus, we denote the Kth user as the *eavesdropper*, and the 2nd to the $(K-1)$ users as the *cooperators*. The information of the 1st user should be perfectly recovered at the 1st receiver. The precoding and decoding matrices of the 1st user cannot be changed according to IA when designing the CES. Some of the cooperators should also sacrifice their own QoS of transmission to make it feasible. The (G+2)th to the (K-1)th users can decode their own information free of interference while facilitating the eavesdropping by the Kth receiver, $1 \leq G \leq K-2$. The lower bound of G will be derived in Section IV-C. The remaining G cooperators, i.e., the 2nd to the $(G+1)$th users, will sacrifice the QoS of their own transmission to help the eavesdropper.

[1]The proposed CES in IA-based networks can be easily extended to asymmetric networks. To do this, for the precoding and decoding matrices, an iterative algorithm can be utilized as in Section III-B. For the feasibility condition, we can refer to (5) in [7] by checking the total number of equations and the total number of variables using a case-by-case method.

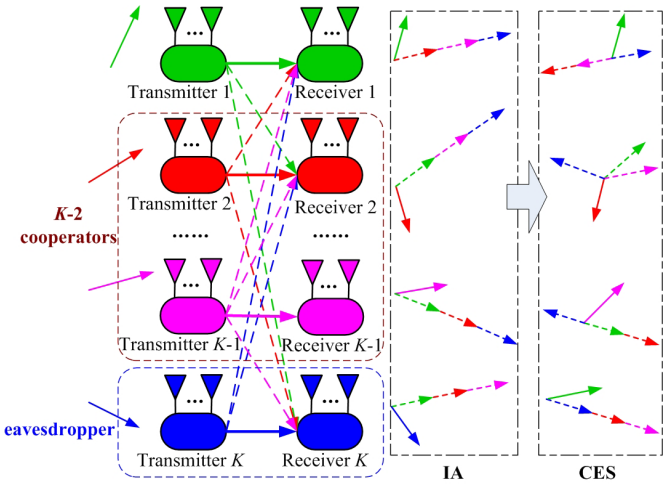

Fig. 3. Demonstration of the CES in IA-based Networks. The 1st user is eavesdropped by the Kth user with the help of the 2nd to the $(K-1)$th users .

Based on the above analysis, some requirements of the CES should be satisfied as follows.

1) The data streams transmitted by the 1st user can be decoded by the receiver of eavesdropper perfectly.
2) The 1st user is not aware of the collusive eavesdropping by the cooperators and eavesdropper.
3) The transmission of the $(G+2)$th to the $(K-1)$th users is carried out free of interference.
4) The interference at the 2nd to the $(G+1)$th receivers is not aligned; nevertheless, their received signal-to-interference-plus-noise ratio (SINR) should be maximized.
5) The data transmission of cooperators and eavesdropper should not stop; otherwise, the 1st user will suspect that it may be eavesdropped.

In the proposed CES, the precoding and decoding matrices of all the users, $\mathbf{V}^{[k]}$ and $\mathbf{U}^{[k]}$, $\forall k \in \{1,2,\ldots,K\}$, are calculated according to the IA principle. Then, the precoding and decoding matrices of the cooperators and eavesdropper are re-designed as $\widehat{\mathbf{V}}^{[j]}$ and $\widehat{\mathbf{U}}^{[j]}$, $\forall j \in \{2,\ldots,K\}$, without being noticed by the 1st user.

To satisfy requirement 1), the signals from the cooperators and eavesdropper should be constrained into the same subspace at the receiver of eavesdropper as Fig. 3. Thus, the following conditions should be satisfied as

$$\widehat{\mathbf{U}}^{[K]\dagger}\mathbf{H}^{[Kj]}\widehat{\mathbf{V}}^{[j]} = \mathbf{0}_{d\times d},\ \forall j \in \{2,\ldots,K\}. \tag{7}$$

According to requirements 2) and 5), the subspace in which the interferences are aligned should not be changed at the 1st receiver, and the transmission of cooperators and eavesdropper should not be terminated; otherwise, the eavesdropping will be noticed. Thus, the following conditions should be abided by

$$\mathbf{U}^{[1]\dagger}\mathbf{H}^{[1j]}\widehat{\mathbf{V}}^{[j]} = \mathbf{0}_{d\times d},\ \forall j \in \{2,\ldots,K\}. \tag{8}$$

When requirement 3) is considered, the interference from other users should be aligned at the $(G+2)$th to the $(K-1)$th receivers, respectively, and their transmission can be performed free of interference. Thus we should follow the conditions as

$$\widehat{\mathbf{U}}^{[i]\dagger}\mathbf{H}^{[i1]}\mathbf{V}^{[1]} = \mathbf{0}_{d\times d},\ \widehat{\mathbf{U}}^{[i]\dagger}\mathbf{H}^{[ij]}\widehat{\mathbf{V}}^{[j]} = \mathbf{0}_{d\times d},$$
$$\forall i \in \{G+2,\ldots,K-1\},\ \forall j \in \{2,\ldots,K\},\ j \neq i. \tag{9}$$

According to requirement 4), the interference at the 2nd to the $(G+1)$th receivers is not aligned, and thus $\widehat{\mathbf{U}}^{[j]}$ is not involved when the other precoding and decoding matrices of the 2nd to the Kth users are re-designed, $\forall j \in \{2,\ldots,G+1\}$. Nevertheless, $\widehat{\mathbf{U}}^{[j]}$ should be calculated according to the re-designed precoding matrices, to maximize their SINR. The SINR of the lth data stream at the jth receiver, $\forall j \in \{2,\ldots,G+1\}$, when considering the residual interference from other users, can be denoted as

$$\mathrm{SINR}^{[jl]} = \frac{P_t^{[j]}}{d}\cdot\frac{\widehat{\mathbf{U}}_{\star l}^{[j]\dagger}\mathbf{H}^{[jj]}\widehat{\mathbf{V}}_{\star l}^{[j]}\widehat{\mathbf{V}}_{\star l}^{[j]\dagger}\mathbf{H}^{[jj]\dagger}\widehat{\mathbf{U}}_{\star l}^{[j]}}{\widehat{\mathbf{U}}_{\star l}^{[j]\dagger}\mathbf{B}^{[jl]}\widehat{\mathbf{U}}_{\star l}^{[j]}}, \tag{10}$$

where

$$\begin{aligned}\mathbf{B}^{[jl]} =& \sum_{i=2}^{K}\frac{P_t^{[i]}}{d}\sum_{m=1}^{d}\mathbf{H}^{[ji]}\widehat{\mathbf{V}}_{\star m}^{[i]}\widehat{\mathbf{V}}_{\star m}^{[i]\dagger}\mathbf{H}^{[ji]\dagger}\\ &+\frac{P_t^{[1]}}{d}\sum_{m=1}^{d}\mathbf{H}^{[j1]}\mathbf{V}_{\star m}^{[1]}\mathbf{V}_{\star m}^{[1]\dagger}\mathbf{H}^{[j1]\dagger}\\ &-\frac{P_t^{[j]}}{d}\mathbf{H}^{[jj]}\widehat{\mathbf{V}}_{\star l}^{[j]}\widehat{\mathbf{V}}_{\star l}^{[j]\dagger}\mathbf{H}^{[jj]\dagger}+\sigma_n^2\mathbf{I}_N.\end{aligned} \tag{11}$$

For any given vector $\widehat{\mathbf{V}}_{\star l}^{[j]}$, the optimal decoding vector to maximize $\mathrm{SINR}^{[jl]}$ can be calculated as [38]

$$\widehat{\mathbf{U}}_{\star l}^{[j]} = \frac{\left(\mathbf{B}^{[jl]}\right)^{-1}\mathbf{H}^{[jj]}\widehat{\mathbf{V}}_{\star l}^{[j]}}{\left\|\left(\mathbf{B}^{[jl]}\right)^{-1}\mathbf{H}^{[jj]}\widehat{\mathbf{V}}_{\star l}^{[j]}\right\|}. \tag{12}$$

Thus $\widehat{\mathbf{U}}^{[j]}$ can be obtained by combining the vectors obtained in (12), $\forall j \in \{2,\ldots,G+1\}$.

Based on the conditions (7)-(9) and the equation (12), the precoding and decoding matrices of cooperators and eavesdropper can be changed without being noticed by the 1st user to satisfy requirements 1) to 5), due to the fact that the interference at the 1st receiver can also be perfectly eliminated through $\mathbf{U}^{[1]}$ according to IA. How to re-design these matrices will be discussed in Section III-B. In summary, the proposed CES in IA-based Networks can be described in Algorithm 1.

B. Iterative Algorithm for the CES

In Section III-A, the CES is proposed to collusively eavesdrop the 1st user in the IA-based network without being noticed by it; nevertheless, how to re-design the precoding and decoding matrices of cooperators and eavesdropper has not been demonstrated. In [5], a MinIL algorithm is proposed, which is an effective method to obtain the solutions of IA iteratively. The MinIL algorithm can also be leveraged to re-design the matrices of cooperators and eavesdropper in the CES, with some necessary modifications. Thus, we first

Algorithm 1 CES in IA-based Networks

1: A time slot starts.
2: The precoding and decoding matrices $\mathbf{V}^{[k]}$ and $\mathbf{U}^{[k]}$ are obtained using the minimizing interference leakage (MinIL) algorithm [5], $k = 1, 2, \ldots, K$.
3: The precoding and decoding matrices of cooperators and eavesdropper, $\widehat{\mathbf{V}}^{[j]}$ and $\widehat{\mathbf{U}}^{[j]}$, are re-designed according to the conditions (7)-(9) and equation (12) without being noticed by the 1st user, $j = 2, 3, \ldots, K$.
4: Transmission begins, and the information of the 1st user is eavesdropped by the Kth user.
5: After a period of T, the time slot ends, and the algorithm goes back to Step 1.

present expressions of the interference covariance matrices used in the algorithm.

In the forward direction, the interference covariance matrices can be defined as

$$\mathbf{Q}^{[k]}=\frac{P_t^{[1]}}{d}\mathbf{H}^{[k1]}\mathbf{V}^{[1]}\mathbf{V}^{[1]\dagger}\mathbf{H}^{[k1]\dagger}+\sum_{\substack{j=2,\\ j\neq k}}^{K}\frac{P_t^{[j]}}{d}\mathbf{H}^{[kj]}\widehat{\mathbf{V}}^{[j]}\widehat{\mathbf{V}}^{[j]\dagger}\mathbf{H}^{[kj]\dagger},$$
$$\forall k \in \{G+2, \ldots, K-1\}, \tag{13}$$

$$\mathbf{Q}^{[K]} = \sum_{j=2}^{K}\frac{P_t^{[j]}}{d}\mathbf{H}^{[Kj]}\widehat{\mathbf{V}}^{[j]}\widehat{\mathbf{V}}^{[j]\dagger}\mathbf{H}^{[Kj]\dagger}. \tag{14}$$

In (14), the signal from the 1st user is not considered in $\mathbf{Q}^{[K]}$, this is because the signal from the 1st user should be eavesdropped rather than eliminated at the eavesdropper. Thus we can compute the decoding vector $\widehat{\mathbf{U}}_{\star l}^{[k]}$ for the lth data stream at the kth receiver as

$$\widehat{\mathbf{U}}_{\star l}^{[k]} = \nu_l\left[\mathbf{Q}^{[k]}\right], l = 1, \ldots, d, \tag{15}$$

where $k \in \{G+2, \ldots, K\}$. The matrix of $\widehat{\mathbf{U}}^{[k]}$ can be obtained through stacking the vectors of $\widehat{\mathbf{U}}_{\star l}^{[k]}$, $k \in \{G+2, \ldots, K\}$.

In the reverse direction, the interference covariance matrices can be defined as

$$\overleftarrow{\mathbf{Q}}^{[k]}=\frac{P_t^{[1]}}{d}\overleftarrow{\mathbf{H}}^{[k1]}\overleftarrow{\mathbf{V}}^{[1]}\overleftarrow{\mathbf{V}}^{[1]\dagger}\overleftarrow{\mathbf{H}}^{[k1]\dagger}+\sum_{\substack{j=G+2,\\ j\neq k}}^{K}\frac{P_t^{[j]}}{d}\overleftarrow{\mathbf{H}}^{[kj]}\overleftarrow{\widehat{\mathbf{V}}}^{[j]}\overleftarrow{\widehat{\mathbf{V}}}^{[j]\dagger}\overleftarrow{\mathbf{H}}^{[kj]\dagger},$$
$$\forall k \in \{2, \ldots, K-1\}, \tag{16}$$

$$\overleftarrow{\mathbf{Q}}^{[K]}=\frac{P_t^{[1]}}{d}\overleftarrow{\mathbf{H}}^{[K1]}\overleftarrow{\mathbf{V}}^{[1]}\overleftarrow{\mathbf{V}}^{[1]\dagger}\overleftarrow{\mathbf{H}}^{[K1]\dagger} + \sum_{j=G+2}^{K}\frac{P_t^{[j]}}{d}\overleftarrow{\mathbf{H}}^{[Kj]}\overleftarrow{\widehat{\mathbf{V}}}^{[j]}\overleftarrow{\widehat{\mathbf{V}}}^{[j]\dagger}\overleftarrow{\mathbf{H}}^{[Kj]\dagger}, \tag{17}$$

where $\overleftarrow{\mathbf{H}}^{[ij]} = \mathbf{H}^{[ji]\dagger}$, $\overleftarrow{\widehat{\mathbf{V}}}^{[k]} = \widehat{\mathbf{U}}^{[k]}, k \neq 1$, and $\overleftarrow{\mathbf{V}}^{[1]} = \mathbf{U}^{[1]}$. Thus we can compute the decoding vector $\overleftarrow{\widehat{\mathbf{U}}}_{\star l}^{[j]}$ for the lth data stream at receiver j as

$$\overleftarrow{\widehat{\mathbf{U}}}_{\star l}^{[j]} = \nu_l\left[\overleftarrow{\mathbf{Q}}^{[j]}\right], l = 1, \ldots, d, \tag{18}$$

where $j \in \{2, \ldots, K\}$. The matrix of $\overleftarrow{\widehat{\mathbf{U}}}^{[j]}$ can be obtained through stacking the vectors of $\overleftarrow{\widehat{\mathbf{U}}}_{\star l}^{[j]}$, $j \in \{2, \ldots, K\}$, and we can set $\widehat{\mathbf{V}}^{[j]} = \overleftarrow{\widehat{\mathbf{U}}}^{[j]}$, $\forall j \in \{2, \ldots, K\}$.

Therefore, we can utilize an iterative algorithm to re-design the precoding and decoding matrices of the cooperators and eavesdropper for the CES to satisfy the conditions of (7) to (9), which is similar to the MinIL algorithm in [5] and hence will not be presented in detail here. For the decoding matrices of the 2nd to the $(G+1)$th users, we can calculate them according to (12).

In the MinIL algorithm [5], the interference covariance matrix is first calculated at each receiver in the forward direction, and the decoding matrix for each user can be obtained by combining the d eigenvectors of the covariance matrix with the smallest eigenvalues. Then, the interference covariance matrix is calculated at each transmitter in the reverse direction, and the precoding matrix for each user can be obtained by combining the d eigenvectors with the smallest eigenvalues. The iterations continue between the forward and reverse directions until it converges. While for the CES, the precoding and decoding matrices of cooperators and eavesdropper are re-designed after the initial legitimate IA scheme. When the matrices are re-designed, it is similar to the MinIl algorithm. The only difference is that the interference covariance matrices in the forward direction use (13) and (14), and the covariance matrices in the reverse direction use (16) and (17) instead.

In most existing research works, the users in the IA-based network are assumed to be authenticated. This is an important assumption to achieve IA, due to the fact that the users should exchange CSI and design the precoding and decoding matrices cooperatively and altruistically. Nevertheless, this is an optimistic assumption when some users in the IA-based network can no longer be trusted[2]. In this case, the untrusted users can collusively eavesdrop other users without being noticed. Thus, the proposed CES can provide a potential threat to IA-based networks, and its analysis will help us to prevent this kind of eavesdropping attack when we design IA networks.

In addition, the proposed CES can be utilized in the cognitive radio or D2D networks, in which the unlicensed or D2D users can act as the eavesdropper and cooperators, to collusively eavesdrop the transmission of the licensed or cellular user. Thus, we pay attention to the design of IA-based cognitive radio or D2D networks, to avoid such adversarial eavesdropping.

IV. Feasibility Condition and Performance Analysis of CES

In this section, the feasibility condition of the proposed CES is presented first, and then the received power of eavesdropping with different numbers of receiving antennas and the minimal number of the low-SINR cooperators are analyzed.

[2]A similar case in which the users in the network cannot be trusted is that some selfish secondary users in a cognitive radio network may send false sensing data to the access point in cooperative spectrum sensing to maximize their benefits [39].

A. Feasibility Condition of CES

The CES in IA-based networks is proposed in Algorithm 1. However, when IA is feasible, how many cooperators can still transmit data to their corresponding receivers free of interference in the CES? In feasible IA-based networks, the number of each user's data streams should satisfy $d \leq \min\{M, N\}$ [7]. Thus, we will derive the feasibility condition of the proposed scheme when $d < \min\{M, N\}$ in this subsection. The special case of $d = \min\{M, N\}$ will be discussed in Section IV-B.

The feasibility condition of IA was analyzed in [7]. A generic polynomial system is solvable if and only if the number of variables is larger than or equal to that of equations. Thus, for a given IA system, it can be classified as either proper or improper based on the number of equations and variables. Nevertheless, proper is not always equivalent to feasibility, and the connection between them is related to the number of data streams transmitted by each user.

Before discussing the feasibility of the proposed CES in IA-based networks, three lemmas in [7] are first recalled[3].

Lemma 1: The total number of equations in (2) of the IA-based network can be given as

$$\mathcal{N}_e = \sum_{\substack{k,i \in \{1,2,\ldots,K\} \\ k \neq i}} d^{[k]} d^{[i]}. \tag{19}$$

Lemma 2: The total number of variables in (2) of the IA-based network can be expressed as

$$\mathcal{N}_v = \sum_{k=1}^{K} d^{[k]} (M^{[k]} + N^{[k]} - 2d^{[k]}). \tag{20}$$

Lemma 3: A symmetric IA system is proper if and only if $\mathcal{N}_v \geq \mathcal{N}_e$.

According to Lemma 1 to Lemma 3, the symmetric IA problem is proper if and only if

$$dK(M + N - 2d) \geq d^2 K(K - 1), \tag{21}$$

and it can be rewritten as

$$d \leq \frac{M + N}{K + 1}. \tag{22}$$

The proper condition (22) of symmetric IA system is achieved only considering (2) without involving (3), because (3) will be satisfied automatically if the channel matrices do not have any special structure.

In the proposed CES for IA-based networks, the conditions (7) to (9) should be satisfied to derive its feasibility condition. The total number of equations in (7) to (9) is demonstrated in Lemma 4.

Lemma 4: The total number of equations in (7) to (9), $\mathcal{N}_e$, can be calculated as

$$\mathcal{N}_e = (K - 1)(K - G)d^2. \tag{23}$$

Proof: According to Lemma 1, the number of equations (7), (8) and (9) is $(K-1)d^2$, $(K-1)d^2$ and $(K-1)(K-G-2)d^2$, respectively.

[3]Detailed explanation on Lemma 1 and Lemma 2 can be found in [7].

Therefore, the total number of equations in (7) to (9) can be expressed as

$$\begin{aligned} \mathcal{N}_e &= (K-1)d^2 + (K-1)d^2 + (K-1)(K-G-2)d^2 \\ &= (K-1)(K-G)d^2. \end{aligned} \tag{24}$$

■

The total number of variables in (7) to (9) is obtained in Lemma 5.

Lemma 5: The total number of variables in (7) to (9) $\mathcal{N}_v$ can be calculated as

$$\mathcal{N}_v = (K-1)(M+N-2d)d - G(N-d)d. \tag{25}$$

Proof: According to Lemma 2, the total number of variables of $\widehat{\mathbf{V}}^{[k]}$ and $\widehat{\mathbf{U}}^{[k]}$ of the cooperators and eavesdropper with $\mathbf{V}^{[1]}$ and $\mathbf{U}^{[1]}$ fixed is $(K-1)(M+N-2d)d$, $\forall k \in \{2, 3, \ldots, K\}$.

However, $\widehat{\mathbf{U}}^{[j]}$, $\forall j \in \{2, \ldots, G+1\}$, is calculated according to (12) after the other precoding and decoding matrices are obtained, whose number of variables is $G(N-d)d$.

Therefore, the total number of variables when the proper condition of the proposed CES is derived can be calculated as $\mathcal{N}_v = (K-1)(M+N-2d)d - G(N-d)d$. ■

According to Lemma 4 and Lemma 5, the proper condition of the proposed CES in IA-based networks is proved in Theorem 1.

Theorem 1: In a feasible IA-based network with $M+N = d(K+1)$ and $d < \min\{M, N\}$, the feasibility condition of the symmetric CES can be expressed as

$$(K-1)(M+N-2d) - G(N-d) \geq (K-1)(K-G)d. \tag{26}$$

Proof: According to Lemma 3 to Lemma 5, we can know that the symmetric CES is proper if and only if

$$\begin{aligned} &\mathcal{N}_v \geq \mathcal{N}_e \Rightarrow \\ &(K-1)(M+N-2d) - G(N-d) \geq (K-1)(K-G)d. \end{aligned}$$

In a feasible IA-based network with $M + N = d(K+1)$ and $d < \min\{M, N\}$, according to the relationship between proper and feasibility, we can know that (26) is the feasibility condition of the proposed CES. ■

Remark 1: Feasibility Conditions and Proper Conditions

- $d = 1$: When only one data stream is transmitted for each user in the IA-based network, i.e., $d = 1$, the proper condition of IA in (22) is equivalent to the feasibility condition in [7]. This is because the polynomial system with independent random coefficients is "generic" in this condition.
- $d \geq 2$: When more than one data streams are transmitted for each user in the IA-based network, i.e., $d \geq 2$, the proper condition of IA in (22) is not always equivalent to the feasibility condition. Nevertheless, most of the proper systems are feasible when (22) is satisfied with only a few counter-examples. Readers are referred to [7] for a detailed discussion of feasibility of proper IA networks with multiple streams, which will not be repeated here to save space. Fortunately, the iterative MinIL algorithm in [5] can be adopted as a theoretical tool for examining

the feasibility of a proper IA network.

- Theorem 1 for CES: In the proposed CES, the collusive eavesdropping is performed based on a feasible IA network, i.e., Theorem 1 is obtained according to an IA network that is already feasible. Thus, in Theorem 1, the feasibility condition (26) can be derived for the CES, whether $d = 1$ or $d \geq 2$, based on a feasible IA network. On the other hand, if we do not have the assumption of a feasible IA network, (26) in Theorem 1 is only a proper condition, which should be further verified by the MinIL algorithm when $d \geq 2$.

B. Received Power of Eavesdropping

In Theorem 1, the feasibility condition of CES to achieve (7) to (9) is derived, which will guarantee interference mitigation at each receiver; however, the received power of the eavesdropping is not analyzed, which is also an important aspect to guarantee the quality of eavesdropping. Before discussing this topic, we introduce Proposition 1 to analyze the received power at a specific receiver in an IA-based network.

Proposition 1: In a feasible IA-based network with $M + N = d(K+1)$, the expectation of the received signal's power at the kth user equals to $dP_t^{[k]}$.

Proof: Since it only concentrates on the condition in (2) without considering $\mathbf{H}^{[kk]}$ in (3) when designing $\mathbf{V}^{[k]}$ and $\mathbf{U}^{[k]}$ for the kth user in a feasible IA-based network, $\mathbf{V}^{[k]}$ and $\mathbf{U}^{[k]}$ are i.i.d., and independent of $\mathbf{H}^{[kk]}$. Therefore $\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\mathbf{V}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{U}^{[k]}$ follows $\mathcal{CW}_d(d, \mathbf{I}_d)$ according to the properties of Wishart matrix [40]. Therefore, the expectation of the received signal's power at the kth user can be expressed as

$$\mathbb{E}\left[\frac{P_t^{[k]}}{d} Tr\Big(\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\mathbf{V}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{U}^{[k]}\Big)\right] = dP_t^{[k]}. \quad (27)$$

■

According to the CES described in Algorithm 1, the received signal's power at the 1st user, and the $(G+2)$th to the $(K-1)$th users, can be expressed as (27) in Proposition 1. However, the received signal's power from the 1st user at the eavesdropper will be changed because of different values of N, and we discuss this as follows.

1) $N = d$

In the CES based on a feasible IA network with $M + N = (K+1)d$ and $N = d$, we have

$$\mathbf{U}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]} = \mathbf{0}_{d\times d}. \quad (28)$$

Since $\mathbf{U}^{[K]}$ is a $d \times d$ unitary matrix when $N = d$, it is also invertible. Thus, we can obtain

$$\mathbf{H}^{[K1]}\mathbf{V}^{[1]} = \Big(\mathbf{U}^{[K]\dagger}\Big)^{-1}\mathbf{U}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]} = \mathbf{0}_{d\times d}. \quad (29)$$

Based on (29), we have

$$\widehat{\mathbf{U}}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]} = \mathbf{0}_{d\times d}, \quad (30)$$

which means that the received signal's power from the 1st user at the eavesdropper is 0, even when the feasibility condition in Theorem 1 can be met.

This special case can also be explained through the idea of a generic polynomial system. When $d = N$, the total number of variables of all the decoding matrices at the receivers is 0 according to Lemma 2. This means that the interference at the receivers of the IA network are all zero-forced by the precoding matrices at the transmitters, and thus the interference can be avoided even without the decoding matrices. Therefore, at the eavesdropper, although the signals from the cooperators and the transmitter of the eavesdropper can be effectively eliminated, the signal from the 1st user is also zero-forced to 0. The information of the 1st user cannot be eavesdropped at the eavesdropper even when the proposed CES is feasible.

2) $N = Kd$

In the CES based on a feasible IA network with $M + N = (K+1)d$, $N = Kd$ and $M = d$, we can obtain the following expression as

$$\mathbf{U}^{[K]\dagger}\mathbf{H}^{[K1]} = \mathbf{U}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]}\Big(\mathbf{V}^{[1]}\Big)^{-1} = \mathbf{0}_{d\times d}, \quad (31)$$

in which $\mathbf{V}^{[1]}$ is also a unitary matrix. Thus, we know that $\mathbf{V}^{[1]}$ is independent of $\mathbf{H}^{[K1]}$. Besides, $\widehat{\mathbf{U}}^{[K]}$ is designed according to (7) to eliminate the signal from the 2nd to the Kth transmitters, and it is also independent of $\mathbf{H}^{[K1]}$. According to Proposition 1, the eavesdropped power of the 1st user at the eavesdropper, when $N = Kd$, can also be expressed as

$$\mathbb{E}\left[\frac{P_t^{[1]}}{d} Tr\Big(\widehat{\mathbf{U}}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]}\mathbf{V}^{[1]\dagger}\mathbf{H}^{[K1]\dagger}\widehat{\mathbf{U}}^{[K]}\Big)\right] = dP_t^{[1]}, \quad (32)$$

due to the fact that $\widehat{\mathbf{U}}^{[K]}$ and $\mathbf{V}^{[1]}$ are i.i.d., and independent of $\mathbf{H}^{[K1]}$.

This special case can also be explained using the idea of a generic polynomial system. When $d = M$, the total number of variables in all the precoding matrices at the transmitters is 0 according to Lemma 2. This means that the received interferences need not be aligned at the receivers of the network using the precoding matrices, and the interferences can be reduced only by the decoding matrices at the receivers directly without any iterations. Therefore, at the eavesdropper, the information of any other user in the feasible IA network can be eavesdropped free of interference by carefully designing its decoding matrix, without the help of any cooperators.

3) $d < N < Kd$

When $d < N < Kd$, both $\mathbf{U}^{[K]}$ and $\mathbf{V}^{[1]}$ will affect $\mathbf{U}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]} = \mathbf{0}_{d\times d}$, and both of them are no longer independent of $\mathbf{H}^{[K1]}$. Besides, $\widehat{\mathbf{U}}^{[K]\dagger}$ is always independent of $\mathbf{V}^{[1]}$ and $\mathbf{H}^{[K1]}$ with different values of N. Thus, when N becomes smaller, $\mathbf{V}^{[1]}$ will act as a more important role in the zero-forcing of (28) than $\mathbf{U}^{[K]}$, which will make the power of the eavesdropped signal from the 1st user, $\widehat{\mathbf{U}}^{[K]\dagger}\mathbf{H}^{[K1]}\mathbf{V}^{[1]}$, become smaller. When $N = d$, the smallest value of N will make the eavesdropped power close to 0; when $N = Kd$, the largest value of N will achieve the largest power of eavesdropping as analyzed in (32).

To further explain the influence on the eavesdropped power due to N, the received signal's power at the 1st user and the

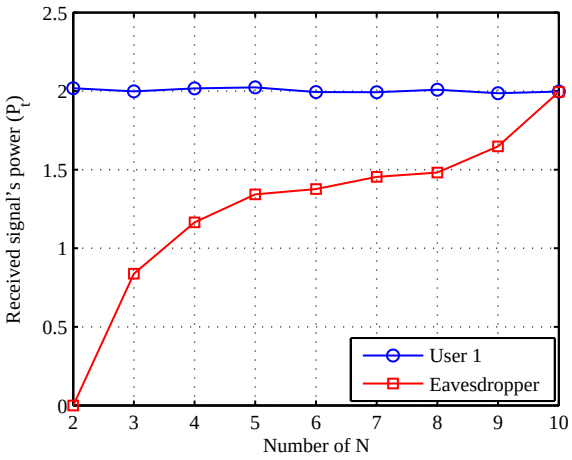

Fig. 4. Received signal's power at the 1st user and the eavesdropper with different values of N, in the CES based on an IA network with $K = 5$, $M + N = 12$, $d = 2$ and $G = 2$.

eavesdropper is shown in Fig. 4 with different values of N in the CES based on an IA network with $K = 5$, $M + N = 12$, $d = 2$ and $G = 2$. The transmitted power of each user is set to P_t. From the results, it is shown that the received signal's power at the 1st user is unchanged and equal to $2P_t$ with different values of N, which is consistent with the analysis of Proposition 1. The eavesdropping power from the 1st user at the eavesdropper increases from 0 to $2P_t$ when N is changed from 2 to 10.

In the CES based on a feasible IA network with $M + N = d(K + 1)$, the number of antennas at each receiver N can range from d to Kd, with two extreme cases of $N = d$ and $N = Kd$. When $N = d$, the re-designed decoding matrix of the eavesdropper $\widehat{\mathbf{U}}^{[K]}$ fails to function, and the received power from the 1st user by the eavesdropper equals to zero, due to the fact that it is only determined by the precoding matrix of the 1st user $\mathbf{V}^{[1]}$ in the initial IA process. When $N = Kd$, the precoding matrix of the 1st user $\mathbf{V}^{[1]}$ in the initial IA process takes no effect, and the received power from the 1st user by the eavesdropper can be expressed in (27) as that in the conventional IA network, due to the fact that it is only determined by the re-designed decoding matrix of the eavesdropper $\widehat{\mathbf{U}}^{[K]}$. As N becomes larger from d to Kd, the influence from the precoding matrix of the 1st user $\mathbf{V}^{[1]}$ in the initial IA process on the received power from the 1st user by the eavesdropper becomes weaker and weaker, which will result in larger received power from the 1st user. The above analysis can be observed in Fig. 4.

Therefore, to guarantee the efficiency of eavesdropping, N should be set as large as possible on condition that the feasibility condition of CES can be satisfied.

C. Discussion of G

Based on Theorem 1, the lower bound of G to make the CES feasible can be derived in Proposition 2.

Proposition 2: Based on a feasible IA network of $M+N = (K+1)d$, the lower bound of G to make the CES also feasible can be expressed as

$$G \geq \begin{cases} 0, & d = M < N, \\ \left\lceil \dfrac{Kd-d}{Kd-N} \right\rceil > 1, & d < \min(M,N), \\ +\infty, & d = N < M. \end{cases} \tag{33}$$

Proof: In a feasible IA network with $M+N = (K+1)d$ and $d < \min\{M, N\}$, from Theorem 1 we can know that the proposed CES is also feasible when

$$(K-1)(M+N-2d) - G(N-d) \geq (K-1)(K-G)d.$$

Therefore, we know that the feasibility condition of the proposed CES can be changed into

$$\begin{aligned} &(K-1)((K+1)d-2d) - G(N-d) \geq (K-1)(K-G)d \\ &\Rightarrow G \geq \left\lceil \frac{Kd-d}{Kd-N} \right\rceil \geq \frac{Kd-d}{Kd-N}. \end{aligned} \tag{34}$$

Based on the analysis in Section IV-B, when $d = M < N$, the information of the 1st user can be easily overheard at the eavesdropper without the help of any cooperators, and we can have the lower bound of G as 0 in this case.

On the other hand, when $d = N < M$, the information of the 1st user cannot be obtained at the eavesdropper because it has already been zero-forced by the precoding matrix of the 1st transmitter, and we can know that the 1st user cannot be eavesdropped no matter how large G is in this case.

Thus, the lower bound of G can be derived as

$$G \geq \begin{cases} 0, & d = M < N, \\ \left\lceil \dfrac{Kd-d}{Kd-N} \right\rceil > 1, & d < \min(M,N), \\ +\infty, & d = N < M. \end{cases}$$

■

Thus, according to Proposition 2, the lower bound of G for the proposed CES is derived, which means that at least G cooperators as indicated in (33) should sacrifice their QoS to help the Kth receiver eavesdrop the 1st user when the CES if feasible.

Remark 3: In a symmetric feasible IA-based networks with $M + N = (K + 1)d$ and $d < \min\{M, N\}$, when N becomes smaller, the number of the low-QoS cooperators G also becomes smaller in the CES. Therefore, smaller N will give more benefit of the cooperators to achieve feasibility. On the other hand, when N becomes smaller, the received power of eavesdropping will be decreased, which will also affect the quality of eavesdropping according to Section IV-B. In addition, there are two special cases of $d = \min\{M, N\}$. When $d = M < N$, the eavesdropper can obtain the information of the 1st user without the help of any cooperators; when $d = N < M$, the eavesdropper cannot overhear the 1st user at all no matter how large G is.

From Proposition 2, we can know that the CES with $M + N = (K + 1)d$ and $d < \min\{M, N\}$ may become infeasible when N is larger. We present Corollary 1 to show the lower and upper bounds of N to make the CES feasible when $d < \min\{M, N\}$.

Corollary 1: Based on a feasible IA network of $M+N = (K+1)d$ and $d < \min\{M, N\}$, when the CES is feasible, the

value of N should satisfy

$$N_{min} = d+1 \leq N \leq \left\lfloor Kd - d - \frac{d}{K-2} \right\rfloor = N_{max}. \quad (35)$$

Proof: From Proposition 2, we can know that G should satisfy the following condition when the CES is feasible with $M+N=(K+1)d$ and $d < \min\{M,N\}$.

$$G \geq \frac{Kd-d}{Kd-N}.$$

We can also know that G should not be larger than $K-2$ when the CES is feasible. When $G=K-2$, it means that all the cooperators should sacrifice their own QoS to help the eavesdropper. Thus, we have

$$\frac{Kd-d}{Kd-N} \leq G \leq K-2. \quad (36)$$

Based on (36), we can obtain

$$N \leq \left\lfloor Kd - d - \frac{d}{K-2} \right\rfloor = N_{max} \leq Kd - d - \frac{d}{K-2}. \quad (37)$$

Besides, according to (33), N should be set larger than d to make the CES feasible, thus we can obtain the lower and upper bounds of N as in (35). ■

From Corollary 1, we can know that N should not be larger than N_{max} (except for the case of $N=Kd$ and $M=d$), when we want to make the CES based on a feasible IA network with $M+N=(K+1)d$ also feasible.

V. Numerical Results and Discussions

In this section, simulation results are provided to show the effectiveness of the proposed CES, and then, the methods for IA to avoid CES and open research challenges are discussed.

A. Numerical Results

In the simulation, we first consider the CES based on an IA network with $K=5$, $d=2$ and $M+N=12$, which is feasible for IA according to its proper condition given in Lemma 3. All the channels suffer from slow Rayleigh block fading as described in (1), and perfect CSI is assumed to be available at each node. Transmit SNR is taken as the metric to measure the quality of the channel, which means the ratio between the transmit power and the background noise. MinIL algorithm [5] is leveraged to calculate the solutions of IA before performing the CES.

The transmission rate of the 1st user, average rate of cooperators, and eavesdropping rate of the eavesdropper, in the CES based on an IA network with two low-QoS cooperators ($G=2$), are compared in Fig. 5 when N equals to 6 and 7. From the results, we can see that the transmission rate of the 1st user and the eavesdropping rate of the eavesdropper when $M=6$ and $N=6$ are much higher than those when $M=5$ and $N=7$. This is because when N is larger than 6, the CES becomes unfeasible according to Theorem 1. Besides, the average transmission rate of the cooperators with $N=6$ is a litter lower than that with $N=7$ when SNR is low, and is a litter higher than that with $N=7$ when SNR is high. This is due to the infeasibility and the higher capacity in maximizing SINR when $N=7$.

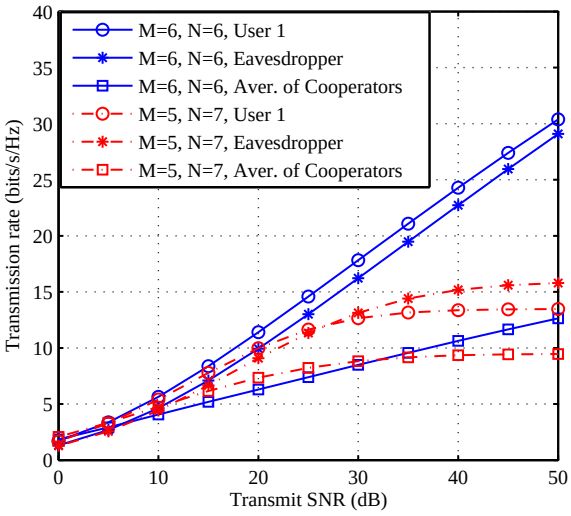

Fig. 5. Comparison of transmission rate of the 1st user, average rate of cooperators, and eavesdropping rate of the eavesdropper, in the CES based on an IA network with $K=5$, $M+N=12$, $d=2$ and $G=2$.

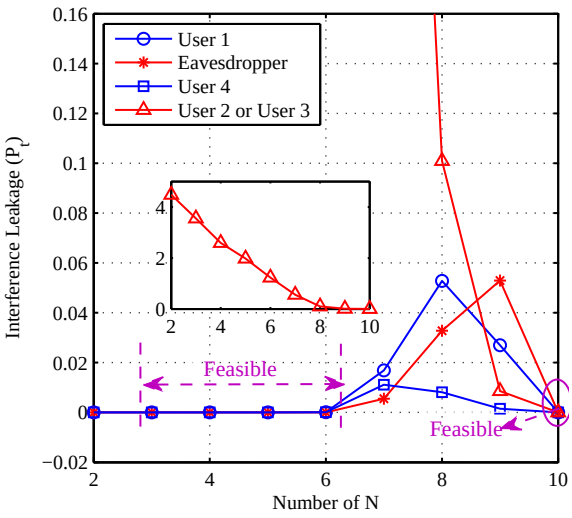

Fig. 6. Interference Leakage comparison of the users with different values of N in the CES of an IA network with $K=5$, $M+N=12$, $d=2$ and $G=2$.

As discussed in Section IV-A and IV-B, the performance of the CES mainly depends on the feasibility of the scheme and the received power of eavesdropping, thus the interference leakage at the users and the transmission and eavesdropping rate of the CES are shown in Figs. 6 and 7 with different values of N, respectively. P_t is the transmitted power of each user, and G is set to 2.

From the results in Fig. 6, we can see that the interference leakage at the 1st user, the 4th user and the eavesdropper is close to zero when $2 \leq N \leq 6$ and $N=10$, which is consistent with Theorem 1. When $7 \leq N \leq 9$, the interference leakage at these users is no longer zero. Besides, from the subfigure inside Fig. 6, we can see that the interference leakage at the other cooperators (user 2 and user 3) are decreasing with

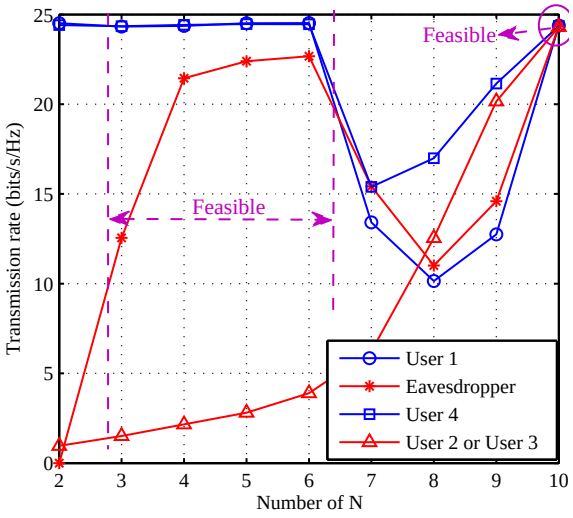

Fig. 7. Comparison of the transmission rate of the 1st user, the average rate of cooperators, and the eavesdropping rate of the eavesdropper, with different values of N, in the CES of an IA network with $K = 5$, $M+N = 12$, $d = 2$ and $G = 2$. SNR=40dB

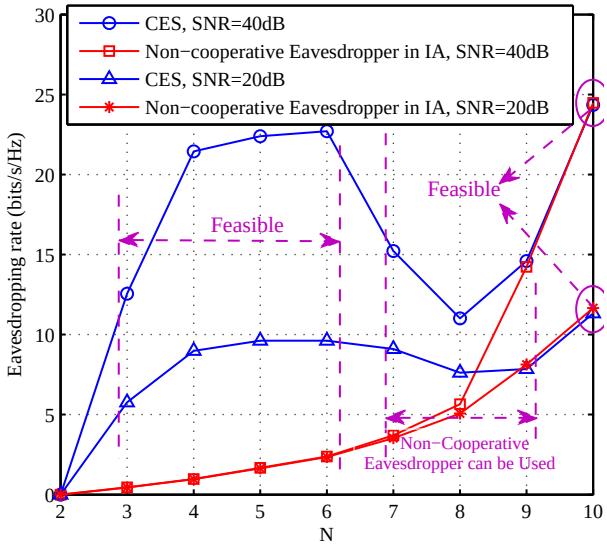

Fig. 8. Eavesdropping rate comparison of the proposed CES and non-cooperative eavesdropper with different values of N in an IA network with $K = 5$, $M + N = 12$, $d = 2$ and $G = 2$.

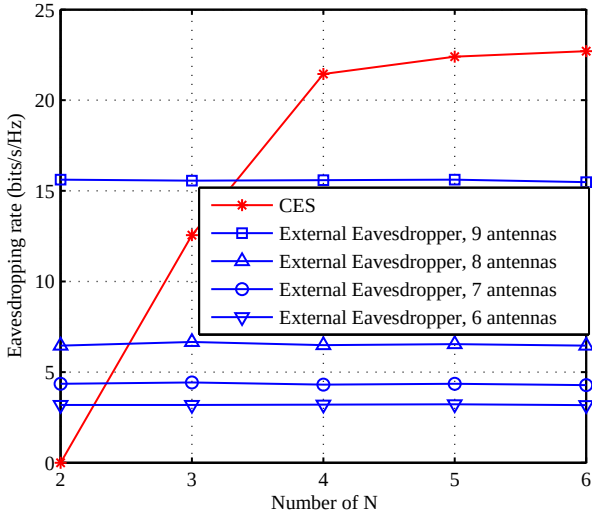

Fig. 9. Eavesdropping rate comparison of the proposed CES and an external eavesdropper with different values of N in an IA network with $K = 5$, $M + N = 12$, $d = 2$ and $G = 2$. SNR=40dB.

larger N. This is because more receiving antennas will make the interference leakage at the cooperators smaller according to (10)-(12). In Fig. 7, SNR is set to 40 dB. From the results, it is shown that the transmission rate of the 1st user and the 4th user is close to 25 bits/s/Hz when $2 \leq N \leq 6$ and $N = 10$, and becomes smaller when $7 \leq N \leq 9$, which is consistent with Theorem 1. The eavesdropping rate at the eavesdropper becomes larger when N increases from 2 to 6, decreases when $7 \leq N \leq 9$, and becomes almost 25 bits/s/Hz when $N = 10$, which is the same as that of the 1st user and the 4th user with $N = 10$. This is because the received power of eavesdropping becomes larger when N increases, which can also be seen in Fig. 4. When $N = 2$, the eavesdropping rate is zero, which is consistent with the analysis of Section IV-B. The average rate of the cooperators becomes larger when N increases, because more receiving antennas will result in lower interference leakage according to (10)-(12). Therefore, based on the results of Figs. 6 and 7, we can know that the CES of an IA network with $K = 5$, $M + N = 12$, $d = 2$ and $G = 2$ is feasible when $3 \leq N \leq 6$ and $N = 10$.

To compare the performance of the proposed CES and the non-cooperative eavesdropping in the IA network, the eavesdropping rate of the CES and a non-cooperative eavesdropper with different values of N is compared in Fig. 8. The non-cooperative eavesdropper, which can be a certain receiver in the IA network, utilizes only decoding matrices to maximize SINR and performs passive eavesdropping similar to the Eavesdropper 1 in Fig. 1. From the results, we can see that, when $3 \leq N \leq 6$, the eavesdropping rate of the CES is much higher than that of the non-cooperative eavesdropper, and becomes close to that of the non-cooperative eavesdropper, when $7 \leq N \leq 8$. When $9 \leq N \leq 10$, the eavesdropping rate of the CES and the non-cooperative eavesdropper is almost the same. Nevertheless, the interference at the 1st user is not eliminated and may be perceived when $7 \leq N \leq 9$, and thus the non-cooperative eavesdropping can be utilized instead of the CES when $7 \leq N \leq 9$.

To compare the performance of the proposed CES and the external eavesdropping in the IA network, the eavesdropping rate of the CES and an external eavesdropper with different values of N is compared in Fig. 9 with SNR=40 dB. The external eavesdropper is similar to the Eavesdropper 3 as in Fig. 1, which performs passive eavesdropping to maximize the SINR through decoding matrices. The CSI of the external eavesdropper is not available in the IA network. The best case of the external eavesdropper is assumed, and the global CSI of the IA network and the number of data streams of each legitimate user can be known by the external eavesdropper. From the results, we can see that when there are 6 antennas equipped at the external eavesdropper, the eavesdropping rate

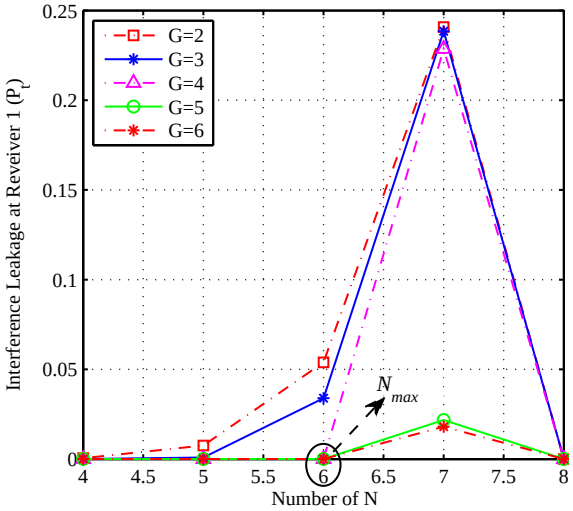

Fig. 10. Interference leakage comparison at the 1st receiver with different values of N and G in the CES of an IA network with $K = 8$, $M + N = 9$, and $d = 1$.

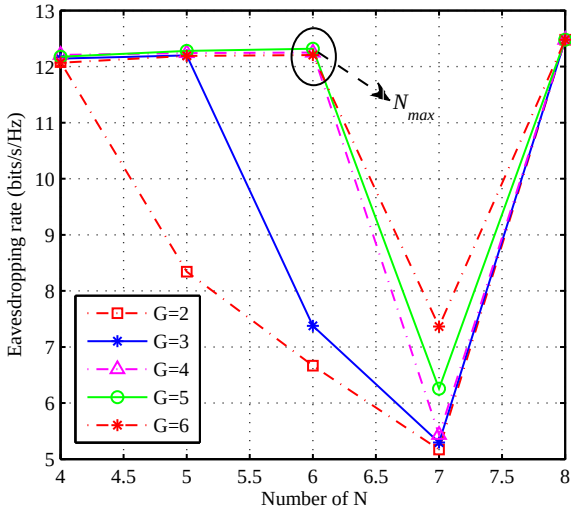

Fig. 11. Eavesdropping rate comparison with different values of N and G in the CES of an IA network with $K = 8$, $M + N = 9$, and $d = 1$.

of the CES is much higher when $3 \leq N \leq 6$, which makes the CES feasible. Nevertheless, the eavesdropping rate of the external eavesdropper becomes higher when more antennas are equipped at the external eavesdropper. Besides, the eavesdropping rate of the external eavesdropper when $N = 2$ is no longer 0, which is higher than that of the CES. To tackle the external eavesdropper, artificial noise can be created by IA users to further prevent the eavesdropping, without influence on the transmission of IA. It will not be discussed in this paper, and we can refer to [37] for more information. In addition, the CSI of the IA network is more easily to be obtained in the CES than the external eavesdropper in practical systems, due to the CSI exchange in IA networks, and thus less CSI is required in the proposed CES.

We then increase the number of users to analyze the maximal value of N, N_{max}, to make the CES feasible in Figs. 10 and 11. In the simulation, $K = 8$, $M + N = 9$, $d = 1$, and SNR=40 dB. First, we compare the interference leakage at the 1st receiver with different values of N and G in Fig. 10. From the results, we can see that, when $G = 2$, the interference leakage is zero when $N \leq 4$; when $G = 3$, the interference leakage is zero when $N \leq 5$; when $4 \leq G \leq 6$, the interference leakage is zero when $N \leq 6$. Then the eavesdropping rate is compared with different values of N and G in Fig. 11. Form the results, it is shown that, when $G = 2$, the eavesdropping rate will not decrease when $N \leq 4$; when $G = 3$, the eavesdropping rate will not decrease when $N \leq 5$; when $4 \leq G \leq 6$, the eavesdropping rate will not decrease when $N \leq 6$. Therefore, based on the results in Figs. 10 and 11, we can achieve the maximal value of N to make CES feasible, N_{max}, is equal to 6, which is consistent with the conclusion of Corollary 1.

B. Methods for IA to avoid CES

In this paper, we have proposed a potential threat for the IA networks, and some methods can be used for the targeted user to avoid this kind of adversarial eavesdropping, some of which are summarized as follows.

(1) In the proposed CES, one certain user is cooperatively eavesdropped by all other users as cooperators and eavesdropper. If there is another user who can be trusted in the IA-based network, i.e., at least two users in the network can be trusted, collusive eavesdropping cannot be performed effectively.

(2) Based on a feasible IA-based network with $M + N = d(K + 1)$, the CES is not always feasible with different numbers of M and N, which is also shown in Theorem 1 and Fig. 6 to Fig. 8. Thus, for the IA users, they can choose some proper values of N to avoid eavesdropping.

C. Open Research Challenges

In Section IV-B, we have concluded that the received signal's power from the 1st user at the eavesdropper will decrease with larger value of N, when the values of K, d and $M + N$ are fixed. In addition, this conclusion has also been verified by several simulation results in Fig. 4, Fig. 7 and Fig. 8. Nevertheless, we cannot present a rigorous proof for this conclusion, which remains an open research challenge in the future.

VI. Conclusions and Future Work

In this paper, we have proposed a novel collusive eavesdropping scheme in IA-based wireless networks. In the proposed scheme, one user is eavesdropped by a eavesdropper with the help of all the other users, which act as cooperators. The precoding and decoding matrices are re-designed to perform the eavesdropping collusively, and thus the user being eavesdropped cannot notice it. To perform the eavesdropping, some of the cooperators should sacrifice their own quality of transmission to help the eavesdropper, and the feasibility condition of the CES was presented. According to the feasibility condition, the minimal number of the low-SINR cooperators and the maximal number of receiving antennas at each receiver

were derived. Besides, the received power of eavesdropping was analyzed with different number of receiving antennas at each receiver, which will also affect the performance of the eavesdropping. Extensive simulation results were presented to show the effectiveness of the proposed CES in IA-based wireless networks. Future work is in progress to further design a novel strategy to improve the eavesdropping performance, in which misleading CSI is fed back to the 1st user by the eavesdropper and cooperators. Besides, an open problem remains to prove that the received power from the 1st user at the eavesdropper will decrease as N becomes smaller.

ACKNOWLEDGMENT

We thank the editor and reviewers for their detailed reviews and constructive comments, which have greatly improved the quality of this paper.

REFERENCES

[1] N. Zhao, F. R. Yu, Y. Chen, B. Chen, and V. C. M. Leung, "Internal collusive eavesdropping of interference alignment networks," in *Proc. IEEE VTC-Spring'17*, pp. 1–6, Sydney, Australia, Jun. 2017.

[2] E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "Evolution towards 5G multi-tier cellular wireless networks: An interference management perspective," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 118–127, Jun. 2014.

[3] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[4] N. Zhao, F. R. Yu, M. Jin, Q. Yan, and V. C. M. Leung, "Interference alignment and its applications: A survey, research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1779–1803, 3rd Quart. 2016.

[5] K. Gomadam, V. R. Cadambe, and S. A. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3309–3322, Jun. 2011.

[6] O. E. Ayach, S. W. Peters, and R. W. Heath, Jr., "The practical challenges of interference alignment," *IEEE Wirel. Commun.*, vol. 20, no. 1, pp. 35–42, Feb. 2013.

[7] C. Yetis, T. Gou, S. A. Jafar, and A. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Proc.*, vol. 58, no. 9, pp. 4771–4782, Sept. 2010.

[8] H. Ning, C. Ling, and K. K. Leung, "Feasibility condition for interference alignment with diversity," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2902–2912, May 2011.

[9] I. Santamaria, O. Gonzalez, R. W. Heath, Jr., and S. W. Peters, "Maximum sum-rate interference alignment algorithms for MIMO channels," in *Proc. IEEE Globecom'10*, pp. 1–6, Miami, FL, Dec. 2010.

[10] B. Xie, Y. Li, H. Minn, and A. Nosratinia, "Adaptive interference alignment with CSI uncertainty," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 792–801, Feb. 2013.

[11] N. Zhao, F. R. Yu, and V. C. M. Leung, "Opportunistic communications in interference alignment networks with wireless power transfer," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 88–95, Feb. 2015.

[12] N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, "A novel interference alignment scheme based on sequential antenna switching in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5008–5021, Oct. 2013.

[13] N. Zhao, F. R. Yu, and H. Sun, "Adaptive energy-efficient power allocation in green interference alignment wireless networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 9, pp. 4268–4281, Sept. 2015.

[14] S. Jafar, "Blind interference alignment," *IEEE J. Sel. Topics Signal Proc.*, vol. 6, no. 3, pp. 216–227, Jun. 2012.

[15] Q. F. Zhou, Q. Zhang, and F. C. M. Lau, "Diophantine approach to blind interference alignment of homogeneous K-user 2x1 MISO broadcast channels," *IEEE J. Sel. Areas. Commun.*, vol. 31, no. 10, pp. 2141–2153, Oct. 2013.

[16] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Proc.*, vol. 59, no. 6, pp. 2783–2794, Jun. 2011.

[17] O. E. Ayach and R. W. Heath Jr., "Interference alignment with analog channel state feedback," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 626–636, Feb. 2012.

[18] H. Gao, T. Lv, D. Fang, S. Yang, and C. Yuen, "Limited feedback-based interference alignment for interfering multi-access channels," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 540–543, Apr. 2014.

[19] N. Zhao, F. Richard Yu, H. Sun, H. Yin, A. Nallanathan, and G. Wang, "Interference alignment with delayed channel state information and dynamic AR-model channel prediction in wireless networks," *Wireless Netw.*, vol. 21, no. 4, pp. 1227–1242, May 2015.

[20] X. Li, N. Zhao, Y. Sun, and F. R. Yu, "Interference alignment based on antenna selection with imperfect channel state information in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5497–5511, Jul. 2016.

[21] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[22] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: pros and cons," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 73–79, Jun. 2015.

[23] A. Mukherjee, S. Ali A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A Survey," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[24] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[25] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[26] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[27] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[28] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sept. 2014.

[29] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[30] Y. Zou, J. Zhu, L. Yang, and Y.-C. Liang, "Securing physical-layer communications for cognitive radio networks," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48–54, Sept. 2015.

[31] H.-M. Wang, C. Wang, D. Ng, M. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.

[32] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.

[33] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, Oct. 2016.

[34] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[35] N. Zhao, J. Guo, F. R. Yu, Ming. Li, and V. C. M. Leung, "Antijamming schemes for interference-alignment-based wireless networks," *IEEE Trans. Veh. Tehnol.*, vol. 66, no. 2, pp. 1271–1283, Feb. 2017.

[36] J. Guo, N. Zhao, F. R. Yu, X. Liu, and V. C. M. Leung, "Exploiting adversarial jamming signals for energy harvesting in interference networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1267–1280, Feb. 2017.

[37] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[38] D. G. Manolakis, V. K. Ingle, and S. M. Kogon, *Statistical and Adaptive Signal Processing: Spectral Estimation, Signal Modeling, Adaptive Filtering and Array Processing*. Boston, MA: McGraw-Hill, 2000.

[39] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, Aug. 2010.

[40] D. K. Nagar and A. K. Gupta, "Expectations of functions of complex Wishart matrix," *Acta Appl. Math.*, vol. 113, no. 3, pp. 265–288, Mar. 2011.

Nan Zhao (S'08-M'11-SM'16) is currently an Associate Professor in the School of Information and Communication Engineering at Dalian University of Technology, China. He received the B.S. degree in electronics and information engineering in 2005, the M.E. degree in signal and information processing in 2007, and the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. His recent research interests include Interference Alignment, Cognitive Radio, Wireless Power Transfer, and Physical Layer Security. He has published more than 100 papers in refereed journals and international conferences.

Dr. Zhao is a senior member of the IEEE and a senior member of the Chinese Institute of Electronics. He is serving or served on the editorial boards of several journals, including Journal of Network and Computer Applications, IEEE ACCESS, Wireless Networks, Physical Communication, AEU-International Journal of Electronics and Communications, Ad Hoc & Sensor Wireless Networks, and KSII Transactions on Internet and Information Systems. He received Top Reviewer Award from IEEE Transactions on Vehicular Technology in 2016, and was nominated as an Exemplary Reviewer by IEEE Communications Letters in 2016. Additionally, he served as a TPC member for many interferences, e.g., Globecom, VTC, WCSP.

F. Richard Yu (S'00-M'04-SM'08) received the PhD degree in electrical engineering from the University of British Columbia (UBC) in 2003. From 2002 to 2006, he was with Ericsson (in Lund, Sweden) and a start-up in California, USA. He joined Carleton University in 2007, where he is currently a Professor. He received the IEEE Outstanding Service Award in 2016, IEEE Outstanding Leadership Award in 2013, Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009 and the Best Paper Awards at IEEE ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009 and Int'l Conference on Networking 2005. His research interests include cross-layer/cross-system design, security, green ICT and QoS provisioning in wireless-based systems.

He serves on the editorial boards of several journals, including Co-Editor-in-Chief for Ad Hoc & Sensor Wireless Networks, Lead Series Editor for IEEE Transactions on Vehicular Technology, and IEEE Transactions on Green Communications and Networking, IEEE Communications Surveys & Tutorials. He has served as the Technical Program Committee (TPC) Co-Chair of numerous conferences. Dr. Yu is a registered Professional Engineer in the province of Ontario, Canada, a Fellow of the Institution of Engineering and Technology (IET), and a senior member of the IEEE. He serves as a member of Board of Governors of the IEEE Vehicular Technology Society.

Yunfei Chen (S'02-M'06-SM'10) received the B.E. and M.E. degrees in electronics engineering from Shanghai Jiao Tong University, Shanghai, China, in 1998 and 2001, respectively, and the Ph.D. degree from the University of Alberta in 2006. He is currently an Associate Professor with the University of Warwick, U.K. His research interests include wireless communications, cognitive radios, wireless power transfer, energy harvesting, channel modeling, SNR estimation, diversity, modulation, and UWB systems.

Victor C. M. Leung (S'75-M'89-SM'97-F'03) received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (UBC) in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at UBC on a Canadian Natural Sciences and Engineering Research Council Postgraduate Scholarship and received the Ph.D. degree in electrical engineering in 1982.

From 1981 to 1987, Dr. Leung was a Senior Member of Technical Staff and satellite system specialist at MPR Teltech Ltd., Canada. In 1988, he was a Lecturer in the Department of Electronics at the Chinese University of Hong Kong. He returned to UBC as a faculty member in 1989, and currently holds the positions of Professor and TELUS Mobility Research Chair in Advanced Telecommunications Engineering in the Department of Electrical and Computer Engineering. Dr. Leung has co-authored more than 1000 journal/conference papers and book chapters, and co-edited 12 book titles. Several of his papers had been selected for best paper awards. His research interests are in the broad areas of wireless networks and mobile systems.

Dr. Leung is a registered Professional Engineer in the Province of British Columbia, Canada. He is a Fellow of IEEE, the Royal Society of Canada, the Engineering Institute of Canada, and the Canadian Academy of Engineering. He was a Distinguished Lecturer of the IEEE Communications Society. He is serving on the editorial boards of the IEEE Wireless Communications Letters, IEEE Transactions on Green Communications and Networking, IEEE Access, Computer Communications, and several other journals, and has previously served on the editorial boards of the IEEE Journal on Selected Areas in Communications C Wireless Communications Series and Series on Green Communications and Networking, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, IEEE Transactions on Computers, and Journal of Communications and Networks. He has guest-edited many journal special issues, and provided leadership to the organizing committees and technical program committees of numerous conferences and workshops. He received the IEEE Vancouver Section Centennial Award and 2011 UBC Killam Research Prize. He is the recipient of the 2017 Canadian Award for Telecommunications Research. He is a co-author of the paper that has won the 2017 IEEE ComSoc Fred W. Ellersick Prize.